SECTION 2
CHAPTER 3
DOCUMENTING CONTROLS

Documenting controls entails documenting the activities and processes for initiating, recording, and reporting transactions for significant accounts and disclosures in order to identify the controls within each process; assessing the effectiveness of the design of the controls to determine whether the controls, as designed, would prevent or detect a material error or misstatement related to an account or groups of accounts; and document the assessment process.

Steps required:

- Document the assessment of effectiveness
- Document the major transaction cycles
- Assess the control environment
- Assess the risk assessment process
- Assess the control activities
- Assess the information and communication processes
- Assess the monitoring processes
- Obtain process owner's concurrence with the documentation of controls

DOCUMENT THE ASSESSMENT OF EFFECTIVENESS

The senior assessment team must document the assessment process of internal control over financial reporting, including[7]:

- The establishment of the senior assessment team, its authority and members;
- Contracting actions if contractors are used to perform or assist in the assessment;
- Communications with agency management and employees regarding the assessment;
- Key decisions of the senior assessment team;
- The assessment methodology and guide;
- The assessment of internal control at the entity level;
- The assessment of internal control at the process, transaction, or application level;
- The testing of controls and related results; and
- Identified deficiencies and suggestions for improvement.

The documentation may be electronic, hard copy format, or both, and should be available for review. Documentation should also include appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls.

DOCUMENT THE MAJOR TRANSACTION CYCLES

Documentation is overseen by the Senior Assessment Team and managed by the Office of Financial Management. Documentation may include narratives, organizational charts, flow charts, questionnaires, decision tables, and memoranda. The first step is documenting the transaction cycles used for each of the significant accounts, groups of accounts, and transactions at bureaus and developing an understanding, from beginning to end, of the underlying processes and document flows involved in each transaction cycle. These are the processes for initiating,

[7] Circular A-123, Appendix A, Section IV.B.

authorizing, recording, processing, and reconciling accounts and transactions that affect the financial reports. The documentation process helps identify the controls that support the assertions made by management related to those accounts or transactions. And it will identify the places in the processes where an error or a misstatement due to error or fraud may occur. Consider multiple controls within the transaction cycle as a single control within a transaction cycle is normally not considered sufficient. Examples of controls that may be identified by management are listed in Addendum B.

To document the Department and bureau's major transaction cycles, gain an understanding of institutional knowledge; examine policy and procedures manuals; gather existing forms and documents; and develop transaction cycle memos (TCMs), process flowcharts, and control matrices. Use the process narrative or the flowchart to document the assessment team's understanding, and then summarize its understanding using the control matrices.

Institutional knowledge. Interviews should be conducted with personnel who have knowledge of the Department and bureau's operations to obtain an understanding of financial and operational business processes. Policy and procedures manuals define the way controls are supposed to function, but interviews with the personnel performing the processes are likely to reveal the way the controls actually operate. Moreover, interviewing the owners of the major classes of transactions may help to identify the controls in place.

Existing policy and procedure manuals. Existing policy and procedure manuals should be reviewed and referred to in the documentation. This is more effective than creating new documentation. If the manuals are obsolete or insufficient, management will be requested by the senior assessment team to update the manuals.

Existing forms and documents. The documentation process includes obtaining examples of the forms and other documents used by the bureau and then highlighting the evidence of controls on each documented example. For example, a person performing a reconciliation usually initials and dates a reconciliation form when he or she completes the reconciliation. Obtain a copy of the form, highlight the evidence of the control activity (e.g., initials and date), and include the form with the documentation. This process will enable the testing of controls, reviewing of project workpapers, and recurring annual assessments to be significantly more efficient.

Some level of documentation of internal controls over financial reporting should be maintained for all locations, including those not considered to be significant either individually or in aggregate. The extent of this documentation may vary across locations, and often is based on the financial significance of each location. This documentation may take many forms, including: policy manuals, accounting manuals, memoranda, flow charts, job descriptions, documents, decision tables, procedural write-ups, self-assessment reports, and other documentation as appropriate. The form and extent of documentation will vary depending on the bureau and office's size, complexity, and documentation approach. However, simply having manuals and policies without demonstration of any reconciliation to the assessment process is not sufficient.

Transaction cycle memos. TCMs provide a written summary describing each transaction's starting point, processing, and completion point. The TCM identifies significant or key controls in the process designed to meet the Department's control objectives and cover management's financial statement assertions. Management relies upon these key controls to prevent and detect material errors and misstatements. Write TCMs ensuring that a reader familiar with internal

controls over financial reporting will understand the process. Since most cycles have many controls, number the controls and identify them by control type. The process owners should review TCMs and ensure that the key controls identified are appropriate and completely address identified risks.

Transaction cycle flowchart. Transaction cycle flowcharts are an efficient way to document key controls in a process, provide basis to confirm the TCMs' accuracy with the process owners, and help identify if more than one control accomplishes the same objective of reducing the risk of an error or misstatement within a process. A flowchart marking key controls with control numbers assigned in the TCM allows comparability with the narrative.

Internal control matrices. Control matrices are an efficient approach to documenting and understanding the key controls and specific risks. A control matrix 1) lists the risks and assertions for an account or line item and the control characteristics that cover the assertions; 2) cross-references the controls to the risks they address; and 3) notes the effectiveness of the process design and operation. It also provides information about the type, level, frequency, objectives, and significance of the controls. This information enables quick determination of an identified risk for which there is no key control. If the risk is determined valid by the process owners, a related control must be present, or there is a gap in internal controls that must be remedied. Refer to Exhibit 1 for a sample internal control matrix.

ASSESS THE CONTROL ENVIRONMENT

The control environment is the organization structure and culture created by management and employees to provide internal control. The control environment is the foundation for all other components of internal control and influences the control consciousness of those working in the organization.

Conduct interviews and surveys to document management's leadership style and the tools management uses to achieve control environment objectives. Automated surveys may help gain a sense of the control environment and point to areas needing additional focus. This serves as evidence of due diligence in assessing the general control environment. A conclusion should indicate whether each of the following aspects of the general control environment is adequate:

- Integrity and Ethical Standards [Integrity, Competence, Attitude, Compliance with Laws]
- Commitment to Competence [Integrity, Competence, and Attitude]
- Management's Relationship with Oversight (Congress, OMB, Etc.)
- Management's Philosophy and Operating Style [Integrity, Competence, and Attitude]
- Organizational Structure [Delegation of Authority and Responsibility]
- Assignment of Authority and Responsibility [Delegation of Authority and Responsibility]
- Human Resource Policies and Practices [Integrity, Competence, Attitude, and Compliance with Laws]
- Compliance with other applicable laws (FMFIA, FFMIA, CFO Act, Inspector General Act of 1978, as amended (IG Act), Financial Information Security Management Act of 2002 (FISMA), Improper Payments Information Act of 2002 (IPIA), Government Performance and Results Act (GPRA), Single Audit Act, as amended, and Clinger-Cohen Act of 1996)

ASSESS THE RISK ASSESSMENT PROCESS

Identify Risk Factors for Financial Reporting. Risk assessment relates to how management considers risks relevant to financial reporting objectives and decides about actions to address those risks. Evaluate management's processes for determining the level of risk related to internal controls over financial reporting and determine actions to address those risks. Starting with the Department's process for complying with GPRA, this includes determining how organization objectives are established, identifies risks that would prevent achievement of the objectives, estimates the significance of the risks in relation to financial reporting, assesses the possible existence of the risks in the current environment, and continues to monitor changes to the environment that may increase or reduce the risks. The results of this assessment at the Departmentwide level will drive the extent of testing and review that needs to be performed at the process, transaction, and application levels.

Consider the following circumstances or events affecting risk:

- Complexity or size of programs, operations, transactions, etc.
- Decentralized versus centralized operations, accounting, and reporting functions
- Extent of manual or automated processes or applications
- New or amended laws, regulations, or accounting standards
- Changes in the operating environment
- Significant new or changed programs or operations
- Restructurings or budget cutbacks which may include downsizing and changes in supervision and segregation of duties
- New personnel or significant personnel changes
- New or revamped information systems
- New technology
- Existence of related party transactions
- Accounting estimates

Prepare a summary of specific risks of misstatement for each significant line item, which will be used to determine the testing plan. The summary should include a list of the significant line items or accounts, related balances and financial statement assertions, and the related risks. Assess the control or combined risk for each assertion, document the assessment, and prepare the testing plan. Refer to Addendum 3 and Exhibit 1 and 2 for additional information and sample templates of the summary of risks.[8]

The types of risks identified may be adapted in determining the testing plan for internal control over financial reporting.

- Inherent risk – the susceptibility of an assertion to misstatement, assuming there are not related specific control activities. Inherent risk factors include: the nature of the Department or bureaus' programs, transactions and accounts and whether the Department had significant audit findings.
- Control risk – the risk that misstatements will not be prevented or detected by the Department or bureaus' internal control (assess separately for each significant financial statement assertion in each significant cycle or accounting application).

[8] Page 19 in CFO Council's *Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A*

- Combined risk – the likelihood that a material misstatement would occur (inherent risk) and not be prevented or detected on a timely basis by the Department or bureaus' internal control (control risk).
- Fraud risk – the risk that there may be fraudulent financial reporting or misappropriation of assets that causes a material misstatement of the financial statements.
- Detection risk – the risk that management will not detect a material misstatement that exists in an assertion.

Identify Control Objectives that Reduce or Eliminate Identified Financial Reporting Risks. Control objectives should address financial processes at each bureau or office. Control objectives are the positive effects that management tries to attain or an adverse condition or negative effect that management seeks to avoid. Controls should provide reasonable, but not absolute assurance of deterring or detecting misuse of resources, failure to achieve program objectives, noncompliance with laws, regulations, and management policies. Controls should be reasonable and weighed against their cost and potential gain. Some control objectives and/or activities that may eliminate or reduce financial reporting risks are:

- Personal integrity and trustworthiness;
- Background investigations and favorable screening;
- Management team that provides continuity and stability;
- Sufficient resources to perform the various job functions;
- Staff possess the requisite knowledge, competencies, and experience;
- Safeguarding of assets and compliance with laws and regulations;
- Physical security/access;
- Segregation of duties;
- Restricted access to resources, records, systems, etc;
- Authorization and approval (supervision) over information and systems;
- Review and reconciliation of financial transactions;
- Transactions and other significant events are well documented in policies and procedures;
- Transactions and events are promptly recorded by authorized persons;
- Adequate internal controls over third party systems or activities;
- Sufficient internal controls in areas that could result in personal gain;
- Adequate training (continuing education) exists that provides staff with technical and ethical training to ensure current knowledge of new rules, regulations, and practices;
- Monitoring of the above control activities to ensure processes, systems and controls are updated and being followed; and
- Sufficient testing to determine whether controls are adequate and consistently applied.

ASSESS THE CONTROL ACTIVITIES

Control activities are policies, procedures, and mechanisms that help ensure the control objectives are met and that management's assertions in the financial reporting are valid. Control activities include preventative or detective controls and may be either manual or automated.

Control activities that may be present include[9]:

- Policies and procedures

[9] Pages 12-16 in GAO's *Standards for Internal Control in the Federal Government* (report AIMD-00-21.3.1), issued November 1999.

- Management objectives
- Top-level reviews of actual performance
- Review and analysis by management at the functional or actual level
- Management of human capital
- Controls over information processing (planning and reporting systems)
- Physical controls over vulnerable assets
- Establishment and review of performance measures and indicators
- Segregation of duties
- Proper execution of transactions and events
- Accurate and timely recording of transactions and events
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control

Reviews by management should be coupled with another control technique to sufficiently mitigate risk. As part of the evaluation, identify any manual controls that are either redundant or secondary to a primary automated control. Redundant and secondary controls that are not effective or not providing the desired level of risk mitigation may be eliminated.

There are three unique elements of control activities that need to be evaluated: information technology controls, third-party service providers, and fraud.

Information technology controls. Interior relies on information technology (IT) controls to perform its missions, manage processes, and report financial information. Evidence that IT system components are operating effectively supports the assessment of internal controls over financial reporting. Applicable system components (e.g. calculations, accumulations, interfaces, and reports) are those affecting significant accounts or disclosures and other relevant financial assertions. Evaluate the following elements of IT controls:

- General IT policies and procedures. General IT policies and procedures are controls relating to key areas like IT strategic planning, budgeting, roles and responsibilities, segregation of duties, resource management, and third-party providers. The Department is integrating the assessment of IT controls as part of the evaluation of internal controls over financial reporting. Compliance with FFMIA and FISMA serve as a foundation for documenting and evaluating the IT controls over financial reporting.
- IT general controls:
  - Systems development and change management. Ensure that IT systems perform their intended functions in an unimpaired manner, free from unauthorized or inadvertent manipulation, and are able to achieve data completeness, accuracy, and timeliness.
  - Availability. Key financial systems subject to outage would adversely affect internal controls because the capability to process, retrieve, and protect data is vital to the Department's ability to accomplish its mission. Key elements related to data availability that need to be considered are business continuity, contingency plans, and environmental and hardware maintenance controls.
  - Information security. The Departmentwide IT security program develops policies, assigns responsibilities, monitors security-related controls, and otherwise manages security risks. Access controls for general support systems and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized alteration, disclosure, loss, or impairment.

- IT automated controls. Include the identification and evaluation of key automated controls during the evaluation of the design and operating effectiveness of key controls. Computerized operations may be assessed further by considering the following factors:
  - Uniform processing of transactions
  - Automatic processing
  - Data validated in real-time or after the transaction was processed
  - Increased potential for undetected misstatements
  - Existence, completeness, and volume of the audit trail
  - Nature of the hardware and software used
  - Unusual or non-routine transactions

Refer to Section 3 for more in-depth information on Interior's IT systems and programs.

Multiple Locations. Interior and its bureaus are comprised of many locations. Stratifying[10] these locations into groups that are expected to behave similarly with respect to audit measures can improve efficiency and the sample results. The stratification should be based on the relative size or qualitative factors such as inherent risk or control risk. If exact information is not available, then estimates may be used. Locations may be stratified into a top, intermediate, and bottom stratum. Criteria for stratifying may include the following factors:

- Amount of assets
- Amounts of revenue or expenses incurred or processed at the location
- Number of personnel, where payroll costs are significant
- Amount of appropriations
- Concentration of specific items (e.g., inventory storage locations)
- Inherent and control risk, including fraud risk and management turnover
- Special reporting requirements (e.g., separate reports, special disclosures)

Third-party service providers. The Department uses internal and external service organizations to process some financial data. These organizations should be evaluated to determine whether the functions performed are significant. If the functions are significant, evaluate evidence describing the operating effectiveness of the provider's controls. Service providers are considered part of Interior's information system when they affect the following:

- The classes of transactions in operations significant to financial reporting.
- The procedures by which transactions are initiated, recorded, processed, and reported from the occurrence to their inclusion in the financial reports.
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial reports involved in initiating, recording, processing and reporting transactions.
- How the Department's information system captures other events and conditions that are significant to the financial reports.
- The financial reporting process used to prepare the Department's financial reports, including significant accounting estimates and disclosures.

A service provider and its auditors issue a report, based on Statement of Auditing Standards No. 70 (SAS 70), Service Organizations. There are two types of reports:

- Type I Report: A Type I report covers the design of a service provider's controls.

[10] GAO's *Financial Audit Manual*, Section 295

- Type II Report: A Type II report covers both the design and the operating effectiveness of the service provider's controls.

If only a Type I report for the service provider is available, tests of the provider's controls must be performed to assess operating effectiveness of the internal controls over financial reporting related to the functions performed by the service provider. A Type II report for the service provider represents additional evidence about the effectiveness of the controls at the service provider as long as the following matters are addressed to satisfaction.

- Type of opinion. If the opinion is not unqualified, obtain an understanding of the nature of the auditor's findings and how these findings may affect the operating effectiveness of Interior's internal controls over financial reporting.
- Period of time covered. The report should cover a sufficient portion of the assessment period to provide evidence of the operating effectiveness for the entire assessment period. If a significant period of time has passed between the end of the time period covered by the service auditor's test of controls and the date of assessment, perform procedures to determine any information in the SAS 70 Type II report in need of update to reflect significant changes in the service organization's controls.
- Scope of the report. Evaluate the report to ensuring coverage of all key controls that need to be tested to provide evidence of the operating effectiveness of internal controls over financial reporting over the functions performed by the service provider.
- Consistency of results with management's review of the service provider. Determine if the results listed in the Type II report are consistent with the results from management's day-to-day review of the accuracy of the service provider.

Fraud. Controls needed to prevent, detect, and correct fraudulent financial reporting should be identified and documented. Normally, these are controls related to estimates and assets that are liquid and more susceptible to misappropriation or theft. Independent verification of and concurrence with the estimating methodology and the data elements of the estimating assumptions are likely to prevent fraudulent financial reporting. Safeguard controls such as restriction of access, requirements for authorizations, and separation of duties may also prevent fraudulent reporting resulting from misappropriation or theft of liquid assets.

Three conditions are generally present when fraud occurs[11]:

- Incentive/Pressure. Management, other employees, or external parties have an incentive or are under pressure, which provides a motive to commit fraud.
- Opportunity. Circumstances exist, such as ineffective or absent controls or the ability of management to override controls that provide an opportunity to commit fraud.
- Attitude/Rationalization. Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

ASSESS THE INFORMATION AND COMMUNICATION PROCESSES

Relevant, reliable, and timely information related to financial reporting should be communicated to relevant personnel at all levels within the Department. To that end, evaluate and document the Department's financial reporting processes to determine what information is based upon

[11] GAO's *Financial Audit Manual*, Section 260

integrated systems or the same source information; whether the information is recorded and communicated in a form and within a time frame that enables managers, operating personnel, and others within the Department who require the information to carry out their internal control, operational, and other responsibilities; and whether the information is made available outside the Department, as appropriate. Documentation should include the evidence reviewed, inquiries performed, and the conclusion as to whether the process is effective. Any aspects of the process found ineffective in the conclusion should be remedied by management. Evaluate the notification to employees of their control-related duties and responsibilities and the manner in which incoming external communications are handled. These responsibilities are usually documented in position descriptions, policy and procedures manuals, written memos and letters that identify and confirm actions taken, meeting agendas, meeting minutes, and oral communications.

ASSESS THE MONITORING PROCESSES

Monitoring the effectiveness of internal control should occur as the normal course of business. Evaluate in what manner the Department and bureaus are monitoring and evaluating the internal control environment and identifying and correcting deficiencies in a timely fashion throughout the year. Consider:

- Ongoing monitoring activities. Look for regular management and supervisory review, comparisons between planned and actual performance, and reconciliations between systems as a part of the regular assigned duties of personnel who affect the Department's financial reporting.
- Performing separate evaluations. Determine processes and resources in place to perform ongoing testing to monitor the operating effectiveness of internal control over financial reporting. Look for inquiries of unusual matters, detail testing of selected transactions, and periodic analysis of trends.
- Reporting deficiencies. Evaluate the process for reporting deficiencies in operating effectiveness to the appropriate level of management, undertaking corrective action in a timely fashion, and tracking the status of corrective actions.

OBTAIN PROCESS OWNER'S CONCURRENCE WITH THE DOCUMENTATION OF CONTROLS

All TCMs, flowcharts, and control matrices should be reviewed and approved by personnel responsible for the respective business processes, transaction cycles, or contract activity. All process owners' comments should be retained and marked to indicate how the comments were resolved. Each comment should result in either a change to the documentation or, if no change occurs, acknowledgement by the process owner that, after further explanation, the comment is not relevant. After addressing the comments, the process owner should sign and date the documentation to show that management has accepted the documentation as a correct representation of the process and controls.